

Before Prediction Becomes Punishment: Governing AI in Bangladesh's Criminal Justice System

Shanjida Israt Jahan Efat

efat@ndub.edu.bd

Notre Dame University Bangladesh

Research Article

Keywords: artificial intelligence, criminal justice, Bangladesh, predictive policing, human rights, algorithmic bias

Posted Date: September 9th, 2026

DOI: <https://doi.org/10.21203/rs.3.rs-10953118/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Additional Declarations: No competing interests reported.

Abstract

Artificial intelligence is entering criminal justice through identification, surveillance, case triage, risk scoring, digital evidence analysis, fraud detection, and prison management. Bangladesh is not starting from a blank page. Its biometric identity infrastructure, the On-site Identification and Verification System used by the Rapid Action Battalion, the 2022 recognition of digital records in evidence law, two national data-governance statutes enacted in 2026, and a draft National AI Policy for 2026–2030 create both capacity and urgency. Yet general commitments to fairness, transparency, and human oversight do not answer the harder question: when, if ever, may an algorithm influence coercive state decisions? This article uses doctrinal and structured comparative policy analysis to examine Bangladesh's constitutional and statutory framework alongside international human-rights standards, selected regulatory models, and empirical research on algorithmic policing and risk assessment. It maps risks across seven points in the criminal justice process and identifies a regulatory gap between data protection and decisional due process. The article proposes a five-gate framework: legal authority, demonstrated necessity, local validity, equality, and effective contestability. Systems failing any gate, it argues, should not help justify arrest, detention, charge, sentence, or release. Lower-risk tools may be introduced through bounded pilots, but only with independent evaluation, public registers, reasoned human decisions, defence access, and sunset clauses. This approach would allow Bangladesh to use AI for social protection and institutional efficiency without converting historical inequality into automated suspicion.

1 Introduction

Artificial intelligence (AI) changes the scale at which criminal justice institutions can classify people. A police officer may once have searched one file at a time. A connected system can now compare a fingerprint with several databases, rank neighbourhoods by predicted crime, identify faces in video, flag financial transactions, summarize case files, or estimate a person's likelihood of reoffending. Some of these uses are administrative. Others can shape arrest, detention, prosecution, sentence, or release. The difference is constitutional, not merely technical.

Bangladesh has reached the moment at which advance rules are still possible. The Rapid Action Battalion introduced an On-site Identification and Verification System (OIVS) in 2021. Public reporting states that the portable system uses a fingerprint to retrieve information from national identity, passport, immigration, criminal, arrest, and prison databases (The Daily Star, 2021). The Evidence (Amendment) Act 2022 brought digital and electronic records within the Evidence Act 1872 and added section 65B on proof of digital records (Government of Bangladesh, 1872/2022). The Personal Data Protection Act 2026 (PDPA) classifies biometric data, information about criminal proceedings or allegations, and real-time geolocation as sensitive personal data, while the National Data Management Act 2026 establishes the institutional structure for national data governance (Government of Bangladesh, 2026a, 2026b). Meanwhile, the National AI Policy Bangladesh 2026–2030, Draft V2.0, treats law enforcement and biometric identification as high-risk, calls for algorithmic impact assessments, and rejects predictive profiling and indiscriminate biometric mass surveillance (ICT Division, 2026). These developments are

not evidence that Bangladesh presently uses automated risk scores in bail or sentencing. They do show that the technical and legal building blocks are converging.

The social stakes are unusually high. Criminal justice data are not a neutral photograph of crime. They record institutional attention: whom police stopped, where patrols were sent, which complaints were believed, and which cases reached court. When these data are reused to predict future risk, an old pattern can become a new instruction. This feedback problem is well documented in predictive policing research (Lum & Isaac, 2016; Richardson et al., 2019). The danger is not confined to race, the category most discussed in North American literature. In Bangladesh, relevant lines of inequality may include sex and gender, poverty, disability, age, religion, ethnicity, place of residence, migration or refugee status, language, political association, and the urban-rural divide. Their effects may overlap.

AI can also serve the public good. It may help find a missing person, expose a trafficking network, detect cyber-fraud, prioritize urgent victim-safety referrals, locate exculpatory material in a large disclosure set, or reduce clerical delay. The proper question is therefore not whether criminal justice should be pro- or anti-technology. It is how law should distinguish assistance from adjudication, investigation from indiscriminate surveillance, and a useful lead from a lawful ground for coercion.

This article develops that distinction for Bangladesh. It makes three contributions. First, it maps AI risk across the criminal justice process rather than treating policing, courts, and corrections as separate digital projects. Second, it connects data-protection rules with the procedural rights triggered when an algorithm materially influences a decision. Third, it offers a five-gate test that public bodies, courts, procurement authorities, and oversight institutions can apply before deployment and throughout a system's life.

The central argument is simple. No algorithm should help justify arrest, detention, charge, sentence, or release unless there is a clear legal basis, a demonstrated and proportionate need, evidence of local validity, an equality assessment, and a practical right to contest the output. Human involvement alone is not enough. A person who merely confirms a score without understanding its limits does not supply meaningful judgment (Green, 2022). The safeguards must therefore reshape institutional practice, not decorate a technical system.

2 Research Questions, Objectives, and Scope

The study addresses four questions:

1. Which present and foreseeable uses of AI in Bangladesh's criminal justice system create the greatest risks to liberty, equality, privacy, dignity, and fair process?
2. To what extent do the Constitution, criminal procedure and evidence law, the PDPA, and the draft National AI Policy govern those risks?

3. What lessons can Bangladesh draw from international human-rights standards, selected regulatory models, and empirical research without importing assumptions from wealthier jurisdictions?
4. What operational safeguards should apply before an AI output may influence a coercive criminal justice decision?

The objectives are to identify the legal and institutional gap; distinguish prohibited, high-risk, and supportive uses; formulate a rights-based decision rule; and propose an achievable implementation sequence. The analysis covers public authorities and private vendors acting for them. It includes police intelligence and resource allocation, biometric identification, investigation and digital evidence, prosecutorial triage, bail and sentencing, prisons and release, victim services, gender-based violence, and cybercrime or financial-crime detection.

The article does not evaluate the source code or accuracy of any specific Bangladeshi system. Nor does it claim that every foreseeable application is currently deployed. Its purpose is anticipatory governance: rules made before a disputed system becomes embedded are usually more effective than remedies developed after harm.

3 Methodology

3.1 Research design and source selection

The article uses doctrinal legal analysis combined with a structured comparative policy review. The research was conducted through 7 September 2026. The domestic corpus comprised the Constitution, the Code of Criminal Procedure 1898, the Evidence Act 1872 as amended in 2022, the Right to Information Act 2009, the Personal Data Protection Act 2026, the National Data Management Act 2026, and Draft V2.0 of the National AI Policy 2026–2030 (Bangladesh Parliament, 2009; Government of Bangladesh, 1872/2022, 1898, 1972, 2026a, 2026b; ICT Division, 2026). Official government texts were preferred. Where an official English translation was not readily accessible, the analysis relied only on propositions that could be confirmed through an official index or a clearly identified translation.

The international corpus included the International Covenant on Civil and Political Rights (ICCPR), the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Convention on the Rights of Persons with Disabilities (CRPD), the United Nations Committee on the Elimination of Racial Discrimination's General Recommendation No. 36, UNESCO's Recommendation on the Ethics of Artificial Intelligence, the Council of Europe Framework Convention on Artificial Intelligence, the OECD AI Principles, and the European Union Artificial Intelligence Act (Committee on the Elimination of Racial Discrimination, 2020; Council of Europe, 2024; European Parliament & Council of the European Union, 2024; OECD, 2024; UNESCO, 2021; United Nations, 1966, 1979, 2006). These materials were selected because they express widely used principles or convert them into risk-based duties. They are not presented as binding on Bangladesh unless Bangladesh is a party to the underlying treaty.

Peer-reviewed and authoritative technical literature was selected around five recurring problems: biased or incomplete data, feedback loops, performance differences across groups, opacity and trade secrecy, and overreliance on nominal human oversight. Recent Asian Journal of Criminology papers were reviewed to situate the article within current debates on facial recognition, AI-enabled regulation, community corrections, and computational criminology (Chen & Dai, 2026; Liu et al., 2026; Lv et al., 2026; Sun et al., 2026).

Comparative materials were used functionally. The inquiry was not which foreign regime Bangladesh should copy, but which safeguard answers a recurring institutional problem. The EU AI Act supplies detailed risk classifications; the Council of Europe Convention connects AI governance to remedies and procedural guarantees; UNESCO supplies an impact-assessment model (UNESCO, 2023); and the Wisconsin Supreme Court's decision in *State v. Loomis* illustrates the difficulty of proprietary risk scoring in sentencing. Each was tested against Bangladesh's constitutional order and administrative capacity.

3.2 Analytical method

Each criminal justice use was assessed against five questions: What legal power authorizes it? What public purpose does it pursue, and could a less intrusive method work? Has it been validated on the local population and intended task? How are errors and benefits distributed? Can an affected person understand, challenge, and obtain review of the result? These questions became the five gates proposed in Section 7.

The analysis distinguishes three kinds of claim. A descriptive claim states what an instrument or study reports. An evaluative claim applies constitutional or human-rights standards to that material. A design recommendation proposes a rule for Bangladesh. This separation is important because international guidance is persuasive, not self-executing domestic law, and evidence from another country may identify a hazard without proving its size in Bangladesh.

3.3 Limitations and use of generative AI

Public documentation of algorithmic tools used by Bangladeshi criminal justice agencies is limited. The absence of a public document is not proof that a system does not exist. Vendor contracts, operational manuals, training datasets, error logs, and disaggregated performance data were generally unavailable. The study therefore does not estimate prevalence, accuracy, or causal effects in Bangladesh. Its proposed safeguards should be tested through consultation with defendants, victims, lawyers, judges, police, prison staff, data-protection specialists, disability organizations, women's rights groups, minority communities, and technical experts.

Generative AI was used for source organization and language assistance. The author independently checked the legal propositions and references, revised the analysis to reflect her own scholarly judgment, and accepts responsibility for the final text. No AI system is listed as an author.

4 Literature Review and Research Gap

4.1 From discretion to datafied discretion

Algorithmic systems do not remove discretion. They redistribute it. Choices made by system designers, data collectors, procurement officers, police supervisors, and frontline users may become less visible than a judge's stated reasons. Brayne's (2017) study of big-data policing found that data systems expanded the scope and automation of surveillance while retaining organizational judgment about what counts as risk. Ferguson (2017) similarly described how network analysis, location forecasting, social-media monitoring, and person-based scoring can alter the grounds on which suspicion is formed.

Risk assessment may improve consistency, but consistency is not the same as justice. Dressel and Farid (2018) found that a widely debated commercial recidivism tool did not outperform untrained human respondents in their experimental comparison and that a simple model using age and prior convictions performed similarly. Chouldechova (2017) demonstrated a deeper mathematical difficulty: where outcome prevalence differs across groups, commonly desired fairness criteria cannot all be satisfied at once. Moreover, apparently neutral variables can reproduce disadvantage through their connection with protected or marginalized groups (Barocas & Selbst, 2016). This does not mean fair decision-making is impossible. It means that a technical team cannot select a fairness metric without making a normative choice about which errors matter and to whom; fairness is a legal and institutional judgment, not a property that software can settle by itself (Wachter et al., 2021).

The same point applies earlier in the process. Predictive policing models trained on recorded drug incidents can direct officers back to locations already subject to enforcement, generating new records that appear to confirm the prediction (Lum & Isaac, 2016). Richardson et al. (2019) call attention to "dirty data": records produced through unlawful or biased practices may contaminate later systems. A model may accurately predict police activity while failing to predict underlying crime.

4.2 Identification, gender, and intersectional error

Biometric systems can assist identification, but their consequences depend on the task. One-to-one verification asks whether a person matches a claimed identity. One-to-many identification searches a probe image against a gallery and produces possible candidates. The latter creates more opportunities for false matches and requires careful threshold setting and human comparison. NIST testing has documented wide variation among face-recognition algorithms and demographic differentials in many systems, though the scale and direction vary by algorithm and application (Grother et al., 2019).

Buolamwini and Gebru (2018) showed intersectional disparities in commercial gender-classification systems, with the poorest performance for darker-skinned women among the groups studied. Gender classification is not facial identification, and the results should not be mechanically transferred. The study nevertheless demonstrates why average accuracy can conceal severe harm for a subgroup. A Bangladeshi evaluation must therefore test people who reflect local variation in skin tone, age, disability, religious dress, gender expression, camera quality, and rural or urban conditions. Categories should not

be treated as biologically fixed. Nor should a system infer gender, ethnicity, religion, emotion, or criminal propensity from appearance.

Gender bias also arises from institutional data. Violence against women is underreported in many settings; complaints may be withdrawn under pressure; and police records may use categories that miss coercive control or technology-facilitated abuse. A model trained only on recorded complaints can mistake low reporting for low risk. Conversely, automated social-media monitoring intended to find abusive content can expose survivors' identities or remove contextual evidence. Protecting victims requires purpose limitation and survivor control, not simply more prediction.

4.3 Opacity, contestability, and the limits of human oversight

Opacity has several sources. A model may be technically complex, a vendor may claim trade secrecy, the data may be inaccessible, or an institution may simply fail to record how a score influenced a decision. In *State v. Loomis* (2016), the Wisconsin Supreme Court allowed limited consideration of a proprietary risk assessment at sentencing but required caution and emphasized that it could not determine sentence by itself. The decision illustrates an unresolved problem: a warning label does not give a defendant the means to test training data, group error, or the logic of an individual result.

Research on sociotechnical systems cautions against isolating the model from the setting in which it operates (Selbst et al., 2019). Human oversight is especially vulnerable to automation bias, time pressure, and unequal access to information. Green (2022) argues that general requirements for a human "in the loop" can legitimize, rather than correct, automated decisions if the reviewer lacks authority, competence, or reasons to depart. Effective oversight therefore requires an identified decision-maker, access to relevant information, power to disregard the output, and a duty to give independent reasons.

Audit is necessary but also incomplete. Internal lifecycle auditing can reveal design and governance failures before deployment (Raji et al., 2020). Independent testing can compare claims with actual performance, while a lifecycle risk-management framework can clarify who must measure and manage risk (National Institute of Standards and Technology, 2023). Neither answers the normative question whether a task should be automated at all. An accurate mass-surveillance system may still be unlawful because its purpose or scale is disproportionate.

4.4 Asian and Global South context

Much algorithmic criminal justice literature originates in the United States and Europe. Its warnings are valuable, but institutional transfer requires care. Global South criminology asks scholars to examine colonial legal histories, informality, unequal state capacity, and locally specific relations between crime, harm, and enforcement (Carrington et al., 2019). Asian criminology likewise contributes by connecting global theory with diverse legal and social settings rather than treating Asia as a testing ground for Northern concepts (Zhang & Liu, 2023).

Recent work in the Asian Journal of Criminology shows both promise and tension. Sun et al. (2026) describe AI-assisted approaches to cyber-fraud and responsive regulation in China and Southeast Asia, while warning that technological enforcement cannot solve the poverty that makes people vulnerable to recruitment. Chen and Dai (2026) explore dilemmas of facial recognition in Chinese digital policing. Lv et al. (2026) examine how AI-mediated community corrections can construct an offender's identity, raising questions about citizenship and control. Liu et al. (2026) demonstrate the value of large language models for structuring Macau judgments while emphasizing validation and selection bias. Together, these papers show that the issue is not simply imported technology. AI becomes part of local institutions, incentives, and ideas about order.

4.5 The Bangladesh gap

Bangladesh's draft AI Policy is notably forward-looking. It calls for human rights, explainability, contestability, risk classification, algorithmic impact assessments, procurement standards, independent oversight, evidence preservation, and redress (ICT Division, 2026). Yet Draft V2.0 still cites the 2025 data-protection and data-governance ordinances that were superseded by Acts Nos. 63 and 80 of 2026. Before adoption, its legal references, institutional roles, and implementation timetable should be conformed to those enacted statutes. UNESCO's national readiness assessment likewise identifies the need to strengthen data-protection and cybersecurity law, build procurement rules, expand diverse Bangla and minority-language datasets, and improve accountability (UNESCO, 2025).

The remaining gap is operational. The PDPA regulates processing and recognizes criminal, biometric, and real-time location data as sensitive. It provides individual rights and organizational duties, but section 24 creates a broad exemption for processing connected with crime prevention, detection, investigation, or prosecution (Government of Bangladesh, 2026b). That breadth makes independent oversight and criminal-procedure safeguards more, not less, important. Data law does not by itself decide whether a face match is sufficient for arrest, whether a risk score may influence bail, what the defence must receive, or which error rate makes a tool unfit for a particular task. The Constitution protects equality, equal protection, life and personal liberty, safeguards on arrest, fair and public trial, and privacy of home and correspondence (Government of Bangladesh, 1972). Those guarantees need procedures capable of reaching a vendor-built model.

The literature reviewed for this article did not provide a Bangladesh-specific, end-to-end framework connecting constitutional rights, data governance, evidence, procurement, and criminal procedure. That is the gap this article addresses.

5 Sector-by-Sector Risk Analysis

Table 1 maps seven areas. The classification concerns the effect of a tool, not its marketing label. A spreadsheet formula, a rules-based score, and a machine-learning model should face the same safeguards if each materially influences liberty.

Table 1
Criminal justice uses, benefits, and primary risks

Stage	Present or foreseeable use	Potential social benefit	Primary rights risk	Proposed baseline
Police planning	Place-based forecasting, network analysis, incident triage	Allocate limited resources; detect linked incidents	Feedback loops; neighbourhood stigma; political or minority profiling	Never treat predicted location as individualized suspicion; publish data and evaluation rules
Identification	Fingerprint matching, retrospective or live face recognition, cross-database identity checks	Identify missing people, unknown bodies, or a suspect from lawful evidence	False match; mass surveillance; function creep; biometric breach	Judicial or independently authorized use for defined serious cases; human comparison; no arrest on match alone
Investigation and evidence	Video search, transcription, translation, device triage, deepfake detection, generative summaries	Find relevant or exculpatory material; reduce delay	Hallucinated facts; altered provenance; disclosure failures	Preserve original evidence; validate tools; disclose use, error, prompts, and transformations
Charging and prosecution	Case prioritization, offence classification, disclosure review	Consistency; earlier identification of weak cases	Automation bias; hidden policy choices; missed exculpatory evidence	Prosecutor remains accountable; reasons recorded; defence notified of material reliance
Bail and sentencing	Failure-to-appear, violence, or recidivism scores; sentencing analytics	Identify candidates for release or support	Preventive punishment; proxy discrimination; opacity	No aggravating use until statute authorizes and independent local validation exists; never sole or decisive basis
Corrections and release	Classification, placement, services, parole support, monitoring	Match support to need; reduce unnecessary custody	Self-reinforcing labels; collective features; excessive surveillance	Use dynamic, reviewable factors; access and correction rights; no denial based solely on score
Victim and cybercrime services	Risk triage, hotline analysis, fraud alerts, trafficking-network detection, abuse-content tools	Faster protection; disruption before loss; scalable assistance	Survivor exposure; false alerts; exclusion by language or disability	Survivor-centred design; minimum data; human response; protection against punitive reuse

5.1 Police planning and predictive enforcement

Place-based forecasting is often described as less intrusive than person-based prediction. It can still intensify surveillance in communities already overrepresented in police records. More patrols produce more observed minor offences, which produce more records, which can justify more patrols. The model's apparent objectivity may conceal the choice to measure police-recorded incidents rather than victimization or social harm.

Bangladesh should prohibit person-based predictive profiling that assigns criminal risk without individualized evidence. The draft AI Policy already points in this direction by identifying predictive profiling and unitary scoring as unacceptable risks (ICT Division, 2026). Place-based tools should not be allowed to create reasonable suspicion or justify a stop, search, arrest, or surveillance order. If used for resource planning, their inputs should exclude protected traits and carefully scrutinize proxies such as postcode, housing, school, occupation, or family association. Agencies should compare deployment patterns before and after use and publish disaggregated results where publication will not compromise a specific investigation.

Police use of generative AI requires a separate rule. A language model may help translate a complaint or organize notes, but it can produce confidently worded false content and express uncertainty poorly (Autio et al., 2024). No generated narrative should enter a first information report, witness statement, case diary, or application for remand without line-by-line verification by the responsible officer. The original account must remain available. A person should never become a suspect because a generative model supplied a plausible but unsupported connection.

5.2 Identification and biometric systems

OIVS demonstrates the immediate utility of connected identification: it can reduce delay in establishing who a person is and may help identify an unknown body. It also demonstrates function creep. When identity, criminal history, immigration, and custodial records can be retrieved together at the roadside, a verification tool can become a broad intelligence profile. The same report stated that OIVS returns whether a person belongs to the Rohingya community (The Daily Star, 2021). That feature is categorization, not merely identity verification, and raises heightened equality, refugee-surveillance, necessity, and purpose-limitation concerns. Accuracy in matching a fingerprint does not guarantee that every linked record is accurate, current, lawfully accessible, or relevant.

The PDPA provides a starting point because biometrics and criminal data are sensitive. Yet its section 24 exemption for crime prevention, detection, investigation, and prosecution is broad. It should not be treated as an affirmative power to conduct any form of surveillance or as a substitute for constitutional legality, necessity, and proportionality (Government of Bangladesh, 2026b). Operational rules should specify who may query which database, for what purpose, for how long a query log is retained, and how a person can correct a false association.

Live facial recognition in public space creates greater risk than retrospective comparison in a defined investigation. It scans many people who are not suspected. Bangladesh should pause live, remote biometric identification until Parliament provides a precise legal basis and an independent body confirms necessity, proportionality, local performance, watchlist quality, and accessible remedies. Even then, it should be confined to exceptional searches for a named missing person or a person lawfully wanted for a serious offence, with time, place, and deletion limits. Emotion recognition, biometric categorization by ethnicity or religion, and inference of criminal propensity from face, voice, movement, or personality should be prohibited.

5.3 Investigation, digital evidence, and large language models

The Evidence (Amendment) Act 2022 recognizes digital records and provides rules for proving them. AI adds a new layer: the record may be selected, enhanced, transcribed, translated, classified, or generated by a system. A court needs to know what the original evidence was, what transformation occurred, which version of the tool was used, and how error was tested. A polished output should not be mistaken for an authentic source.

For AI-assisted evidence, provenance is the central safeguard. Investigators should preserve the original file, its cryptographic hash where practicable, the chain of custody, system and model version, relevant settings, date and operator, and all material transformations. If a generative system summarized documents, the summary should be treated as an investigative aid, not evidence of its own assertions. Both prosecution and defence should be able to trace a contested statement to the source. Where the system helps identify inculpatory material, an equivalent process should search for exculpatory material.

Deepfake detection illustrates uncertainty. Creation and detection methods develop against each other, so performance may not transfer across manipulation types or operational settings (Mirsky & Lee, 2021). Detection tools may be useful, but they should not reverse the burden of proof or create a presumption that disputed media are authentic. Experts should report validation conditions and confidence, and courts should evaluate the whole evidentiary foundation.

5.4 Prosecution, bail, remand, and sentencing

Algorithmic triage can help a prosecution office find delayed cases or check for inconsistent charging. It becomes dangerous when a score replaces individualized assessment. A model trained on past charging decisions may reproduce unequal access to lawyers, uneven police investigation, or outdated policy. Efficiency cannot justify making an invisible charging policy.

Bail and sentencing require the highest threshold because liberty is immediate and the presumption of innocence is central before conviction. The practical stakes are substantial: the World Prison Brief reported that pre-trial or remand detainees constituted 73.1% of Bangladesh's prison population on 29 November 2025 (Institute for Crime & Justice Policy Research, 2026). Risk scores often rely on age, prior contact, employment, residence, family circumstances, or peer associations. Some variables may predict

an outcome statistically while penalizing poverty or social disadvantage. Youth is a clear example: it may correlate with reoffending while also reducing culpability and increasing capacity for change (Stevenson & Slobogin, 2018).

Bangladesh should initially forbid aggravating use of algorithmic scores in bail, remand, and sentence. A tool may be studied for the limited purpose of identifying people who can safely receive a less restrictive measure, but only in a controlled evaluation and without making another person worse off. Any later use should require legislation, prospective local validation, defence access, a written judicial explanation, and an express rule that the score cannot be the sole or decisive basis. Trade secrecy must yield where disclosure is necessary to challenge a deprivation of liberty. If a vendor will not permit adequate scrutiny, the state should not buy the system.

5.5 Corrections, parole, and rehabilitation

In corrections, risk and need assessments can direct education, treatment, security classification, or release. The same score can either open a service or close a door. That double use should be avoided. A person labelled high-risk may be denied lower security, then denied opportunities available only in lower security, and later be treated as higher-risk because those opportunities were not completed.

The framework should separate needs from dangerousness. Supportive assessments should identify changeable needs and protective factors, not merely deficits. People in custody should be told when a system affects placement, privileges, services, or release; they should see the material inputs, correct errors, and obtain periodic review. Static factors must not make rehabilitation conceptually impossible. Disability should trigger accommodation, not a higher risk label caused by communication differences or unmet support needs.

5.6 Victim protection, gender-based violence, and children

AI can help route urgent hotline calls, detect coordinated harassment, identify repeat perpetrators across complaints, or warn a potential fraud victim before money is transferred. These are strong public-interest uses when designed around assistance. The risk is that a protection tool becomes an enforcement or surveillance tool. A survivor may avoid help if disclosure automatically triggers police action, family notification, immigration consequences, or loss of a device.

Victim-service systems should collect the minimum data needed, state who can access them, and prevent secondary use for unrelated enforcement. Bangladesh's 2024 national survey on violence against women expanded measurement to technology-facilitated gender-based violence and emphasized persistent data gaps affecting marginalized women; that evidence supports survivor-centred, intersectional data governance rather than reliance on police records alone (Bangladesh Bureau of Statistics, 2025). High-risk alerts must reach trained people able to respond safely. Models should be evaluated in Bangla and relevant regional or minority languages and with speech affected by distress or disability. Children require heightened limits: profiling should not follow them into adulthood, and educational or welfare records should not become general police intelligence.

A gender-responsive impact assessment must look beyond whether men and women receive equal error rates. It should ask who is missing from the dataset, whose behaviour is interpreted as suspicious, whose complaint is downgraded, who bears surveillance within a household, and whether a system recognizes transgender and non-binary people without forcing harmful classification. Consultation should be safe, compensated where appropriate, and capable of changing or stopping the project.

5.7 Cybercrime, financial crime, and cross-border cooperation

Fraud and cybercrime detection may offer the clearest near-term benefits. Pattern analysis can flag unusual transactions, connect infrastructure used across scams, and prioritize warnings. Sun et al. (2026) show how AI-assisted financial intelligence and victim-focused prevention may disrupt cyber-fraud, while also emphasizing cross-border limits and social vulnerability.

These systems still require discipline. An alert is a lead, not proof. Financial behaviour may reflect remittance patterns, informal work, disaster response, or limited access to banking. A bank or mobile financial service should not freeze funds indefinitely or report a person as criminal solely because of an opaque model. Rules should provide rapid human review, notice when it will not compromise an investigation, and compensation for avoidable loss. Cross-border data exchange should record purpose, recipient, retention, security, and onward-transfer limits.

6 Findings: What the Existing Framework Provides and What It Misses

The analysis produces five main findings.

First, Bangladesh already has a constitutional foundation for regulation. Equality and equal protection (article 27), protection of law (article 31), life and personal liberty (article 32), safeguards on arrest and detention (article 33), fair and public trial (article 35), and privacy of home and correspondence (article 43) do not disappear because a decision is described as data-driven (Government of Bangladesh, 1972). The ICCPR reinforces equality before courts, privacy, effective remedy, and non-discrimination (United Nations, 1966). Its fair-trial guarantee requires practical equality of arms, a principle that is difficult to preserve if the prosecution can rely on a system that the defence cannot meaningfully test (Human Rights Committee, 2007).

Second, the PDPA and National Data Management Act create an important data-governance architecture, but they are not sufficient. The PDPA can govern collection, access, security, retention, and complaints about personal data, although its criminal-justice exemption is wide; the National Data Management Act establishes the responsible national authority (Government of Bangladesh, 2026a, 2026b). Neither statute alone specifies the evidentiary weight of an AI output or the procedural disclosure necessary in a criminal case. Data protection and criminal procedure must be connected.

Third, the draft AI Policy contains many of the right principles but remains a policy draft. It sensibly classifies justice and law-enforcement tools as high-risk, requires impact assessment, and identifies red lines. Its continuing references to superseded 2025 ordinances also create avoidable legal uncertainty. Implementation will depend on alignment with the 2026 Acts, statutory authority, institutional independence, resources, and rules that officials can apply to actual decisions.

Fourth, the most serious risk is cumulative. A mistaken identity may enter a police database, influence a network analysis, shape a charging decision, appear in a bail score, and follow a person into prison classification. Sector-by-sector oversight misses this chain. Audit must follow data and decisions across agencies.

Fifth, "human oversight" is too vague. It is meaningful only where the human reviewer has time, training, information, authority to depart, and a duty to explain. Table 2 summarizes the present baseline and operational gap.

Table 2
Rights baseline and criminal-justice-specific gap

Source	Existing protection	Operational gap for algorithmic criminal justice
Constitution of Bangladesh	Articles 27, 31–33, 35, and 43 protect equality, legality, liberty, arrest safeguards, fair trial, and privacy	No specific notice, disclosure, validation, or remedy rule for algorithmic influence
Code of Criminal Procedure	Judicial control of remand, bail procedure, reasons in specified decisions	Does not define permissible reliance on risk scores or machine-generated information
Evidence Act as amended	Recognition and proof of digital records	Limited guidance on AI transformation, model provenance, generated content, and defence testing
Personal Data Protection Act 2026	Sensitive-data rules, individual rights, security and retention duties; broad section 24 criminal-justice exemption	Data rights may not reveal how a score affected coercive discretion; the exemption requires narrower sectoral safeguards and independent oversight
National Data Management Act 2026	Establishes the national data-governance authority and institutional structure	Does not supply criminal-case rules on algorithmic evidence, decisional weight, disclosure, or remedy
Right to Information Act 2009	General public access framework	Security and investigative exemptions may obstruct system-level transparency; proactive algorithm register is absent
Draft National AI Policy 2026–2030	Risk tiers, AI impact assessments, red lines, oversight, redress	Non-final policy; criminal justice thresholds, courtroom procedure, and institutional allocation are not detailed

7 A Five-Gate Framework for Bangladesh

Every high-risk criminal justice system should pass five cumulative gates before procurement, again before deployment, and periodically during operation. Failure at one gate should stop the use. The burden belongs to the deploying authority, not the affected person.

7.1 Gate 1: Legal authority

The agency must identify a clear, accessible legal power for the particular use, dataset, decision, and information-sharing pathway. A general power to prevent crime or modernize administration is insufficient for mass biometric surveillance or liberty-affecting scoring. The rule should identify the purpose, eligible offences or cases, authorized users, retention, sharing, and oversight. Secret law cannot support foreseeable interference with rights.

7.2 Gate 2: Demonstrated necessity and proportionality

The authority must define the problem with evidence, compare less intrusive alternatives, and specify a measurable benefit. Convenience is not necessity. An impact assessment should consider the number and vulnerability of people affected, seriousness of possible error, duration of impact, possibility of function creep, and whether the system changes the distribution of police attention. A pilot must have stopping criteria and cannot waive fundamental safeguards.

7.3 Gate 3: Local validity and reliability

Performance must be tested on data representative of the intended Bangladeshi population, setting, language, equipment, and task. Evaluation should report false positives and false negatives, calibration, uncertainty, missing data, and performance under realistic conditions. It should compare the system with existing practice and a simpler baseline. Vendor claims or accuracy from another country are not enough. Material updates require revalidation.

7.4 Gate 4: Equality and distribution of error

Aggregate performance must be disaggregated across legally and socially relevant groups, including intersections where sample size permits. Review must examine proxies and institutional bias, not only direct use of protected traits. A disparity requires explanation and mitigation; severe or uncorrectable disparity requires non-deployment. Equality assessment must also ask who receives the benefit. A system that reduces average delay while making legal challenge inaccessible to rural, poor, disabled, or linguistically marginalized people is not equitable.

7.5 Gate 5: Effective contestability and remedy

People must receive timely notice of material algorithmic influence, the purpose of the system, relevant input data, understandable reasons, known limitations, and a route to human reconsideration. In criminal proceedings, the defence should obtain information necessary to test reliability and application, subject to narrowly tailored protective orders where justified. Courts must be able to exclude unreliable outputs and draw appropriate inferences when the state or vendor fails to preserve evidence. Affected people

need correction, deletion where appropriate, review, compensation, and the ability to trigger investigation by an independent body.

Table 3
The five gates in operational form

Gate	Minimum evidence before deployment	Decision if unmet
Legal authority	Published legal basis, purpose, users, data flows, retention, decision role	Do not procure or use
Necessity	Documented problem, alternatives analysis, proportionality assessment, success and stop criteria	Redesign or stop
Local validity	Independent task-specific testing, simple baseline, uncertainty and failure analysis	No operational reliance
Equality	Disaggregated and intersectional testing, proxy review, community input, mitigation	Suspend where serious disparity remains
Contestability	Notice, reasons, logs, defence access, correction, review, remedy, accountable human	Output cannot affect an individual decision

The framework is deliberately stricter than ordinary public-sector automation. Criminal justice combines state coercion, informational inequality, stigma, and sometimes irreversible harm. It also accommodates beneficial tools. A transcription system may satisfy the gates with proportionate testing and source verification. A national person-risk score may fail at the first two.

8 Recommendations and Implementation Roadmap

8.1 Enact a criminal justice algorithmic safeguards chapter

Parliament should enact a dedicated chapter, whether in future AI legislation or coordinated amendments to criminal procedure, evidence, police, prison, and data-protection law. It should define an algorithmic decision system by function and effect; apply to systems developed in-house or bought from vendors; establish the five gates; and create red lines. Prohibited uses should include social scoring for law enforcement, prediction of offending based solely on profiling or personality, biometric categorization by sensitive traits, emotion recognition in interrogation or court, indiscriminate live biometric surveillance, and any automated decision that determines arrest, detention, guilt, sentence, or release without meaningful human judgment.

8.2 Create a public register and procurement rule

The Bangladesh Public Procurement Authority should require an algorithmic schedule for every relevant tender. It should describe intended use, datasets, evaluation plan, audit access, security, intellectual-property limits, update control, incident reporting, exit and deletion, and liability. Contracts must guarantee the state, court, defence under protective conditions, and independent auditor access

sufficient to evaluate a contested system. Procurement should never create a trade-secret barrier to constitutional review.

A public register should list agency, vendor, purpose, decision stage, legal basis, impact-assessment summary, validation status, performance ranges, update dates, complaints, incidents, and suspension. Operational details that would create a concrete investigative risk may be withheld temporarily, but the existence and general function of a rights-affecting system should not be secret.

8.3 Establish independent, plural oversight

Technical coordination and rights oversight should not be located entirely in the deploying ministry. A criminal justice AI oversight panel should include the judiciary, National Human Rights Commission, National Data Management Authority, bar and legal aid representatives, criminologists, statisticians, cybersecurity experts, disability and gender specialists, and community members. Members should disclose conflicts, and affected groups should have more than a ceremonial consultation role.

The panel should approve high-risk pilots, commission testing, receive incident reports, order suspension, and publish annual findings. Courts retain authority over admissibility and legality. Parliamentary committees should review aggregate use, expenditure, and rights impact.

8.4 Build procedural safeguards into cases

Criminal procedure rules should require the prosecution to disclose material algorithmic use, whether the output is inculpatory or exculpatory. The disclosure should cover the system's purpose, input used for the person, output, known limits, validation relevant to the task, and how the official relied on it. Judges should ask whether the five gates were satisfied before giving weight to the output.

For arrest and search, a match or prediction should never be sufficient by itself. For bail, remand, sentencing, and release, no adverse algorithmic assessment should be used until legislation expressly permits the use and independent local validation supports it. A judge must give reasons in ordinary legal terms and identify any reliance. Where the output cannot be adequately tested, it should carry no adverse weight.

8.5 Adopt gender-responsive and accessibility requirements

Impact assessments should include sex, gender, disability, age, language, location, socioeconomic position, and relevant intersections. Evaluation teams should work with organizations serving women and girls, transgender people, persons with disabilities, children, ethnic and linguistic minorities, and refugees. Regional research on AI and gender reinforces the need to examine participation, data gaps, and unequal impact rather than rely on formal neutrality (UNESCO, 2026). Notices and challenge processes must be available in accessible Bangla and, where needed, other languages and formats. Offline routes are essential in light of the digital divide identified in Bangladesh's UNESCO readiness assessment (UNESCO, 2025).

Victim-protection tools require a firewall against unrelated enforcement. Data collected for safety should not be used to punish a survivor, monitor lawful relationships, or initiate unrelated immigration or criminal action except where a clear law and an immediate, serious threat justify it.

8.6 Invest in people and independent evidence

Judges, prosecutors, defence lawyers, police, prison officials, and legal aid providers need role-specific training. Training should not turn every official into a data scientist. It should enable them to ask: What exactly does the output predict? Against what outcome and time period? How often is it wrong? On whom? Has it been tested here? What information is missing? Can I disagree, and must I explain why?

Universities can support independent evaluation through interdisciplinary centres combining law, criminology, statistics, computer science, sociology, and gender studies. Public funding should protect academic independence and support Bangla-language, locally representative research. No operational dataset should be released without privacy and security controls, but controlled research access is preferable to vendor self-certification.

8.7 Use a phased timetable

Table 4
Proposed implementation sequence

Period	Priority actions	Responsible institutions
First 12 months	Inventory systems and contracts; freeze prohibited uses; align the final AI Policy with the 2026 data statutes; issue interim disclosure and provenance rules; create public register; audit OIVS access, categorization, and correction processes	Ministry of Law, Ministry of Home Affairs, ICT Division, judiciary, National Data Management Authority
12–24 months	Enact safeguards; adopt procurement schedule; establish independent panel; develop local test protocols; train judges, lawyers, and officials	Parliament, rule-making bodies, procurement authority, universities and professional bodies
24–36 months	Run bounded low-risk and supportive pilots; publish evaluations; create defence expert-support fund; test complaint and compensation pathways	Deploying agencies, legal aid, oversight panel, courts
Continuing	Annual equality and performance audits; incident reporting; revalidation after updates; three-year sunset review; suspend systems that drift or lose necessity	Oversight panel, Parliament, courts, auditors

The sequence begins with inventory because a state cannot govern systems it has not identified. It prioritizes supportive tools over coercive prediction. Sunset review prevents a pilot from becoming permanent by inertia.

9 Discussion

The proposed framework reframes innovation. In criminal justice, the fastest deployment is not necessarily the most modern policy. A system that cannot explain its legal basis, show local validity, or survive challenge is a source of institutional fragility. It can produce wrongful decisions, contested prosecutions, data breaches, public distrust, and long-term vendor dependence.

The five gates also clarify debates about accuracy. Accuracy is necessary for many uses, but it is not a complete legal test. A highly accurate system can be disproportionate; a moderately accurate supportive tool may be acceptable when a trained person verifies every output and no one is made worse off. The decision must account for purpose, alternatives, error costs, and remedy.

This matters for gender equality. Technical fairness work often asks whether groups receive similar error rates. Law and criminology ask additional questions: Why was this outcome selected? Which conduct has been criminalized or ignored? Did the dataset emerge from equal access to police protection? Does prediction intensify control over people who already have less freedom? These questions cannot be resolved by code alone.

The framework is also responsive to institutional capacity. It does not require Bangladesh to reproduce an expensive foreign regulator before taking any action. An inventory, interim prohibition, procurement clause, written-reasons rule, preserved audit log, and university-supported validation are feasible starting points. At the same time, scarcity cannot excuse experimentation on people facing loss of liberty. Where an agency cannot evaluate a high-risk system, the responsible choice is not to use it for that purpose.

Finally, the article distinguishes prevention from pre-emption. Socially useful prevention reduces opportunities for harm, supports potential victims, addresses vulnerability, and interrupts suspicious transactions with review. Pre-emption assigns suspicion to a person because a system predicts what that person may do. The former can strengthen collective safety. The latter approaches punishment without an act and deserves the law's greatest caution.

10 Conclusion

Bangladesh can still decide what role AI should play in criminal justice before high-risk systems become ordinary. The country has a constitutional rights framework, new data-governance statutes, growing digital infrastructure, and a draft AI Policy that recognizes the danger of predictive profiling and mass surveillance. What it lacks is a bridge from principle to the daily decisions that expose a person to police attention, detention, prosecution, sentence, or continuing control.

The five-gate framework supplies that bridge. Legal authority prevents governance by procurement contract. Necessity separates public need from technological enthusiasm. Local validity rejects borrowed claims of accuracy. Equality makes the distribution and production of error visible. Contestability turns transparency into a usable remedy. Applied together, the gates establish a firm rule: an algorithm that cannot pass them must not make coercion easier.

AI should first be used where it expands protection and reduces avoidable delay: finding relevant evidence, warning potential victims, identifying missing people, improving access to legal information, and directing services. Even there, people need privacy, verification, and redress. The future of criminal justice should not be a choice between inefficient institutions and automated injustice. Bangladesh can pursue a third path: careful innovation under law, open to evidence, and answerable to the people most affected.

Declarations

Author Contribution

The sole author was responsible for conceptualization, methodology, investigation, analysis, writing, review, and editing.

References

1. Autio, C., Schwartz, R., Dunietz, J., Jain, S., Stanley, M., Tabassi, E., Hall, P., & Roberts, K. (2024). *Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile (NIST AI 600-1)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.AI.600-1>
2. Bangladesh Bureau of Statistics (2025). *Bangladesh violence against women survey 2024*. United Nations Population Fund. <https://asiapacific.unfpa.org/en/publications/bangladesh-violence-against-women-survey-2024>
3. Bangladesh Parliament (2009). *Right to Information Act, 2009 (Act No. XX of 2009)*. <https://bdlaws.minlaw.gov.bd/act-1011.html>
4. Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. *California Law Review*, 104(3), 671–732. <https://doi.org/10.15779/Z38BG31>
5. Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review*, 82(5), 977–1008. <https://doi.org/10.1177/0003122417725865>
6. Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of Machine Learning Research*, 81, 77–91. <https://proceedings.mlr.press/v81/buolamwini18a.html>
7. Carrington, K., Dixon, B., Fonseca, D., Goyes, D. R., Liu, J., & Zysman, D. (2019). Criminologies of the Global South: Critical reflections. *Critical Criminology*, 27(1), 163–189. <https://doi.org/10.1007/s10612-019-09450-y>
8. Chen, X., & Dai, M. (2026). Dilemmas of facial recognition technology in Chinese digital policing: A qualitative exploration. *Asian Journal of Criminology*, 21., Article 2. <https://doi.org/10.1007/s11417-025-09473-1>
9. Chouldechova, A. (2017). Fair prediction with disparate impact: A study of bias in recidivism prediction instruments. *Big Data*, 5(2), 153–163. <https://doi.org/10.1089/big.2016.0047>

10. Committee on the Elimination of Racial Discrimination (2020). *General recommendation No. 36 on preventing and combating racial profiling by law enforcement officials (CERD/C/GC/36)*. United Nations. <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-36-2020-preventing-and>
11. Council of Europe (2024). *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)*. <https://rm.coe.int/1680afae3c>
12. Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. *Science Advances*, 4(1), eaao5580. <https://doi.org/10.1126/sciadv.aao5580>
13. European Parliament & Council of the European Union (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. *Official Journal of the European Union* <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
14. Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University.
15. Government of Bangladesh (1872/2022). *The Evidence Act, 1872 (Act No. 1 of 1872), as amended by the Evidence (Amendment) Act, 2022*. <https://bdlaws.minlaw.gov.bd/act-details-24.html>
16. Government of Bangladesh (1898). *The Code of Criminal Procedure, 1898 (Act No. V of 1898)*. <https://bdlaws.minlaw.gov.bd/act-details-75.html>
17. Government of Bangladesh (1972). *The Constitution of the People's Republic of Bangladesh*. <https://bdlaws.minlaw.gov.bd/act-367.html>
18. Government of Bangladesh (2026a). *National Data Management Act, 2026 (Act No. 80 of 2026)*. <https://bdlaws.minlaw.gov.bd/act-1709.html>
19. Government of Bangladesh (2026b). *Personal Data Protection Act, 2026 (Act No. 63 of 2026)*. <https://bdlaws.minlaw.gov.bd/act-print-1692.html>
20. Green, B. (2022). The flaws of policies requiring human oversight of government algorithms. *Computer Law & Security Review*, 45, 105681. <https://doi.org/10.1016/j.clsr.2022.105681>
21. Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face Recognition Vendor Test Part 3: Demographic effects (NISTIR 8280)*. National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.IR.8280>
22. Human Rights Committee (2007). *General comment No. 32: Article 14, right to equality before courts and tribunals and to a fair trial (CCPR/C/GC/32)*. United Nations. <https://www.refworld.org/legal/general/hrc/2007/en/52583>
23. Division, I. C. T., & Government of Bangladesh. (2026).. *National AI Policy Bangladesh 2026–2030 (Draft V2.0)*. <https://aipolicy.gov.bd/docs/national-ai-policy-bangladesh-2026-2030-draft-v2.0.pdf>
24. *World Prison Brief: Bangladesh*. Institute for Crime & Justice Policy Research, & Birkbeck (2026). University of London. Retrieved September 7, 2026, from https://www.prisonstudies.org/country/bangladesh?language_content_entity=en-gb

25. Liu, J., Li, D. M., Ju, Q. R., & Zhang, X. S. (2026). Structuring Macau's criminal court judgments with large language models: Methodological innovations for data accuracy and sample selection bias. *Asian Journal of Criminology*, 21., Article 14. <https://doi.org/10.1007/s11417-025-09475-z>
26. Lum, K., & Isaac, W. (2016). To predict and serve? *Significance*, 13(5), 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960.x>
27. Lv, T., Jiang, J., & Meng, Y. (2026). Digital citizenship or digital bondage: How AI-based technologies construct the identity of offenders within Chinese community corrections. *Asian Journal of Criminology*, 21. <https://doi.org/10.1007/s11417-026-09493-5>. Article 23.
28. Mirsky, Y., & Lee, W. (2021). The creation and detection of deepfakes. *ACM Computing Surveys*, 54(1). <https://doi.org/10.1145/3425780>. Article 7.
29. National Institute of Standards and Technology (2023). *Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1)*. <https://doi.org/10.6028/NIST.AI.100-1>
30. OECD (2024). *Recommendation of the Council on Artificial Intelligence (OECD/LEGAL/0449)*. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>
31. Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* (pp. 33–44). Association for Computing Machinery. <https://doi.org/10.1145/3351095.3372873>
32. Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review Online*, 94, 15–55. <https://www.nyulawreview.org/online-features/dirty-data-bad-predictions/>
33. Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. In *Proceedings of the 2019 Conference on Fairness, Accountability, and Transparency* (pp. 59–68). Association for Computing Machinery. <https://doi.org/10.1145/3287560.3287598>
34. State v. Loomis, 881 N.W.2d 749 (Wis. 2016). <https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html>
35. Stevenson, M. T., & Slobogin, C. (2018). Algorithmic risk assessments and the double-edged sword of youth. *Behavioral Sciences & the Law*, 36(5), 638–656. <https://doi.org/10.1002/bsl.2384>
36. Sun, J., Gu, S., & Su, R. (2026). AI-empowered responsive regulation for preventing future crimes: An empirical inquiry into the regulatory pyramid to combat future crimes in China and Southeast Asia. *Asian Journal of Criminology*, 21, 8. <https://doi.org/10.1007/s11417-025-09477-x>
37. The Daily Star (2021, February 28). Rab launches on-site identification, verification system to check criminal profile instantly. <https://www.thedailystar.net/bangladesh/news/rab-launches-site-identification-verification-system-check-criminal-profile-instantly-2052577>
38. UNESCO (2021). *Recommendation on the Ethics of Artificial Intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000380455>

39. UNESCO (2023). *Ethical impact assessment: A tool of the Recommendation on the Ethics of Artificial Intelligence*. <https://unesdoc.unesco.org/ark:/48223/pf0000386276>
40. UNESCO (2025). *Bangladesh: Artificial Intelligence Readiness Assessment Report*. <https://unesdoc.unesco.org/ark:/48223/pf0000396493>
41. UNESCO (2026). *Outlook study on artificial intelligence and gender in South Asia*. <https://unesdoc.unesco.org/ark:/48223/pf0000398795>
42. United Nations (1966). *International Covenant on Civil and Political Rights*. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
43. United Nations (1979). *Convention on the Elimination of All Forms of Discrimination against Women*. <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-elimination-all-forms-discrimination-against-women>
44. United Nations (2006). *Convention on the Rights of Persons with Disabilities*. <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities>
45. Wachter, S., Mittelstadt, B., & Russell, C. (2021). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. *Computer Law & Security Review*, 41, 105567. <https://doi.org/10.1016/j.clsr.2021.105567>
46. Zhang, J., & Liu, J. (2023). Asian criminology: Its contribution in linking Global North and South. *International Annals of Criminology*, 61(3–4), 223–242. <https://doi.org/10.1017/cri.2023.22>